(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平10－161864

(43)公開日　平成10年(1998)6月19日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　9/06	５５０	Ｇ０６Ｆ　9/06	５５０Ａ
			５５０Ｚ

審査請求　未請求　請求項の数９　ＯＬ　（全 13 頁）

(21)出願番号　特願平8－317917

(22)出願日　平成８年(1996)11月28日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　田中　利清
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

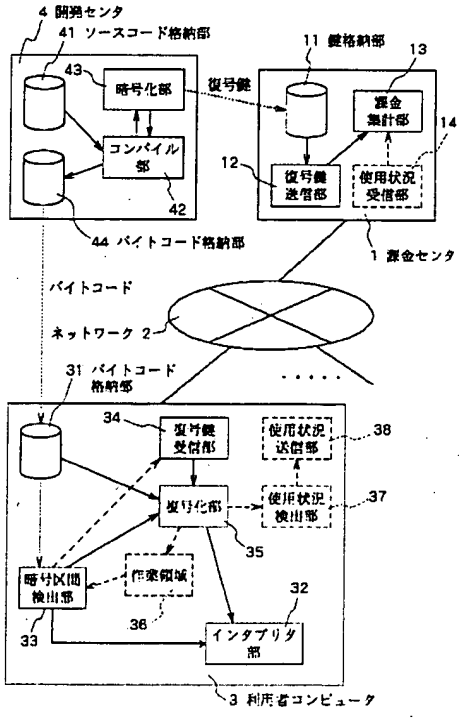
(74)代理人　弁理士　若林　忠

(54)【発明の名称】　ソフトウェアの保護方式

(57)【要約】

【課題】　ソフトウェアの使用機能に着目し、ソフトウエアの使用回数などに応じた使用料の徴収を可能とし、また、不正コピーを防止できる保護方式を提供する。

【解決手段】　ソースコードをコンパイルして得られたバイトコードを利用者コンピュータ３に配布し、利用者コンピュータ３では、バイトコードをインタプリタによって解釈実行するシステムにおいて、配布されるバイトコードの一部を暗号区間として暗号化する。ネットワーク２に接続され暗号区間に対応する復号鍵を保持する課金センタ１を設ける。利用者コンピュータ３には、課金センタ１から復号鍵を取得する復号鍵受信部３４と、配布されたバイトコード中での暗号区間の開始と終了とを検出する暗号区間検出部３３と、復号鍵を用いて暗号区間内のバイトコードを復号する復号化部３５と、復号されたバイトコードを解釈実行するインタプリタ部３２と、を設ける。



【特許請求の範囲】

【請求項１】　ソフトウエアのソースコードをコンパイラにより変換して得られたバイトコードを利用者コンピュータに配布し、前記利用者コンピュータでは、前記バイトコードをインタプリタによって、順次、解釈実行するソフトウエア実行システムにおける、ソフトウエアの保護方式において、

ソフトウエアごとに前記利用者コンピュータに配布されたバイトコードの少なくとも一部の区間が暗号区間として暗号化されており、

前記利用者コンピュータが接続されたネットワークと、

前記ネットワークに接続され前記暗号区間に対応する復号鍵を保持する課金センタとを有し、

前記利用者コンピュータが、前記課金センタから前記復号鍵を取得する復号鍵取得手段と、前記配布されたバイトコード中での前記暗号区間の開始と終了とを検出する暗号区間検出手段と、前記復号鍵を用いて前記暗号区間内のバイトコードを復号する復号手段と、復号手段で復号されたバイトコードを、順次、解釈実行するインタプリタ手段と、を備えていることを特徴とするソフトウエアの保護方式。

【請求項２】　前記利用者コンピュータ内に、当該利用者コンピュータでのソフトウエアの使用を検出して使用記録を保持し、前記使用記録を前記課金センタに送付する使用記録検出手段を有し、

前記課金センタが、送付されてきた前記使用記録に基づいて課金処理を実行する、請求項１に記載のソフトウエアの保護方式。

【請求項３】　前記配布されたバイトコードを前記利用者コンピュータが実行する前に前記復号鍵取得手段が前記課金センタから前記復号鍵を取得し、前記課金センタが前記復号鍵の配布履歴に基づいて課金処理を実行する、請求項１に記載のソフトウエアの保護方式。

【請求項４】　前記配布されたバイトコードに複数の暗号区間が設定されて各暗号区間に暗号区間ＩＤが付与され、前記暗号区間ＩＤごとに復号鍵が対応して前記配布されたバイトコードが複数種類の復号鍵に対応し、

前記復号鍵取得手段が、前記配布されたバイトコードを前記利用者コンピュータが実行する前に前記課金センタから復号鍵を一括して取得するとともに、前記バイトコードの実行中に、前記暗号区間ごとに前記暗号区間ＩＤに基づいて復号鍵の選択を実行する、請求項１乃至３いずれか１項に記載のソフトウエアの保護方式。

【請求項５】　前記配布されたバイトコードに複数の暗号区間が設定されて各暗号区間に暗号区間ＩＤが付与され、暗号区間ＩＤごとに復号鍵が対応して前記配布されたバイトコードが複数種類の復号鍵に対応し、

前記復号鍵取得手段が、前記配布されたバイトコードの実行中に前記暗号区間が検出されるたびに、当該暗号区間の前記暗号区間ＩＤに基づいて前記課金センタから該当する復号鍵を取得し、

前記課金センタが前記復号鍵の配布履歴に基づいて課金処理を実行する、請求項１に記載のソフトウエアの保護方式。

【請求項６】　前記利用者コンピュータ内に、当該利用者コンピュータでのソフトウエアの使用を検出して使用記録を保持し、前記使用記録を前記課金センタに送付する使用記録検出手段を有し、

前記課金センタが、送付されてきた前記使用記録に基づいて課金処理を実行する、請求項５に記載のソフトウエアの保護方式。

【請求項７】　前記利用者コンピュータに作業領域を有し、前記配布されたバイトコードの実行中に前記暗号区間を検出した場合には、当該暗号区間内の全バイトコードをまとめて復号してから、前記インタプリタ手段が当該バイトコードの解釈実行を行う、請求項１乃至６いずれか１項に記載のソフトウエアの保護方式。

【請求項８】　ソフトウエアのソースコードをコンパイラにより変換して得られたバイトコードを利用者コンピュータに配布し、前記利用者コンピュータでは、前記バイトコードをインタプリタによって、順次、解釈実行するソフトウエア実行システムにおける、ソフトウエアの保護方式において、

前記利用者コンピュータが接続されたネットワークと、

前記ネットワークに接続され前記暗号区間に対応する復号鍵を保持する課金センタとを有し、

前記利用者コンピュータ内に、当該利用者コンピュータでのソフトウエアの使用を検出して使用記録を保持し、

前記使用記録を前記課金センタに送付する使用記録検出手段が設けられ、

前記課金センタが、送付されてきた前記使用記録に基づいて課金処理を実行することを特徴とするソフトウエアの保護方式。

【請求項９】　ソフトウエアのソースコードをコンパイル手段により変換して得られたバイトコードを利用者コンピュータに配布し、前記利用者コンピュータでは、前記バイトコードをインタプリタによって、順次、解釈実行するソフトウエア実行システムにおける、ソフトウエアの保護方式において、

前記コンパイル手段は、暗号区間の開始、暗号区間の終了を示すコードが前記ソースコードに存在する場合には、当該コードを暗号区間の開始、暗号区間の終了を示すバイトコードに変換するものであり、

前記暗号区間内のバイトコードを暗号化する暗号化手段をさらに備え、

ソフトウエアごとに前記利用者コンピュータに配布されるバイトコードの少なくとも一部の区間が前記暗号区間として暗号化されていることを特徴とする、ソフトウエアの保護方式。

【発明の詳細な説明】

【０００１】
【発明の属する技術分野】本発明はいわゆる中間コードとしてのバイトコードを使用するソフトウエアに対する保護方式に関し、特に、ソフトウエアの使用量に比例した使用料金の徴収を可能とするソフトウエアの保護方式に関する。
【０００２】
【従来の技術】ソフトウエアの中には、Ｊａｖａアプレットやある種のアプリケーションなど、ソフトウエアの開発時にはコンパイラによりソースコードをバイトコード（中間コード）に変換し、このバイトコードを利用者に配布し、ソフトウエアの実行時にインタプリタによりこのバイトコードを、順次、解釈実行するものがある。この利用者側のコンピュータには、バイトコードを解釈実行するためのインタプリタを予め用意しておくものとする。この方法では、利用者側のコンピュータに要求されるハードウエアがそれほど大きくなくて済む上、配布されるバイトコード自体も比較的コンパクトなため、ネットワークなどの使用を前提として、例えば、ネットワークに接続された多数のコンピュータにソフトウエアを同時にインストールしたりするのに有効な技術として、注目を集めている。
【０００３】ところで、従来、パーソナルコンピュータなどのアプリケーションソフトウエアは、一般に、これらソフトウエアの実行形式プログラムを格納した記録媒体を用いて、買い取り方式により販売されている。しかしながら、買い取り方式では、流通経費を相対的に低減したいという動機づけ（インセンティブ）が働くので、ソフトウエアの機能が必要以上に肥大化し、ほとんど使用しない機能まで含めて利用者は高額の費用を負担せざるを得なくなることが多い。この場合、購入代金は、利用者がそのソフトウエアを実際に使用した頻度によらず、一定である。また、機能が必要以上に肥大化した際には、そのソフトウエアを実行させるために必要なハードウエア量も増大し、動作速度が低下する。さらに、実際にソフトウエアを購入して実行してみなければ、利用者が必要とする機能が満足されているか否かを判断することができない。
【０００４】最近では、買い取り方式の変形として、暗号化したソフトウェアをＣＤ－ＲＯＭなどの記録媒体またはネットワーク経由で配布し、電話、ファクシミリ、手紙（郵送）または電子メールによる購入手続きの後、復号鍵を通知する方式も採用されている。この場合でも、使用回数にかかわらず同一の金額を支払わなければならず、使用回数または使用時間当たりの価格には大きな幅がある。さらにこの方式では、復号したソフトウェアを不正にコピーして使用することを防ぐことができず、著作権者の権利の保護に万全を期することができない。
【０００５】
【発明が解決しようとする課題】以上説明したように、アプリケーションソフトウエアの現行の販売方法では、利用者の側には、不要な機能にまで代金を払っているという不満があり、一方、著作権者の側には権利が十分保護されないという不満がある。
【０００６】本発明の目的は、ソフトウェアの使用機能に着目し、ソフトウエアの使用量、使用回数などに応じた使用料の徴収を可能とするとともに、ソフトウエアの不正なコピーを防ぐことができるソフトウェアの保護方式を提供することにある。
【０００７】
【課題を解決するための手段】本発明のソフトウエア保護方式は、ソフトウエアのソースコードをコンパイラにより変換して得られたバイトコードを利用者コンピュータに配布し、利用者コンピュータでは、バイトコードをインタプリタによって、順次、解釈実行するソフトウエア実行システムにおける、ソフトウエアの保護方式において、ソフトウエアごとに利用者コンピュータに配布されたバイトコードの少なくとも一部の区間が暗号区間として暗号化されており、利用者コンピュータが接続されたネットワークと、ネットワークに接続され暗号区間に対応する復号鍵を保持する課金センタとを有し、利用者コンピュータが、課金センタから復号鍵を取得する復号鍵取得手段と、配布されたバイトコード中での暗号区間の開始と終了とを検出する暗号区間検出手段と、復号鍵を用いて暗号区間内のバイトコードを復号する復号手段と、復号手段で復号されたバイトコードを、順次、解釈実行するインタプリタ手段と、を備えている。
【０００８】すなわち、本発明では、ＣＤ－ＲＯＭやフロッピーディスクなどの記録媒体により、あるいは、ネットワークを介して流通するソフトウエアは、バイトコードであって、その一部がソフトウエア開発時に暗号化されている。そして、課金センタを設けて復号鍵を課金センタで集中して管理し、利用者コンピュータ側からの要求にしたがいネットワークを介して復号鍵が配送される。そして利用者コンピュータとして、バイトコードをインタプリタによって１命令ずつ解釈実行するものを使用する。
【０００９】本発明によれば、バイトコードの一部を暗号化し、復号鍵はその都度配送するようにしてソフトウエアの実行中に復号処理を行うので、いずれの時点においても、利用者コンピュータ側では、復号されたソフトウエアが磁気ディスクなどのファイルシステム内に格納されることがなく、ソフトウエアを不正にコピーして使用することが防止される。
【００１０】課金センタでは、復号鍵の配布履歴に基づき、あるいは、利用者コンピュータ側からネットワークを介して集めた使用記録すなわち使用状況に関するデータに基づいて課金処理を行うことができ、これにより、使用回数などに比例した使用料の徴収が保証される。

【００１１】本発明では、暗号化に使用される暗号鍵としてソフトウェア全体で１つの鍵またはソフトウェアの機能の単位で異なる複数の鍵が使用でき、これら暗号鍵に対応して１あるいは複数の復号鍵が使用される。複数の鍵を使用する場合には、ソフトウェア内の暗号区間の開始を指定するバイトコードのオペランドに暗号区間ＩＤが設定され、暗号区間ＩＤに対応させて復号鍵が管理されるようにすればよい。復号鍵の配送に当たっては、適切な認証および暗号化を実施することが好ましい。

【００１２】

【発明の実施の形態】次に、本発明の実施の形態について、図面を参照して説明する。図１は本発明の実施の一形態のソフトウエアの保護方式の構成を示すブロック図である。

【００１３】このソフトウエアの保護方式では、課金センタ１と利用者コンピュータ（実行マシン）３とが、ネットワーク２を介して接続している。ここでは、利用者コンピュータ３は、アプリケーションソフトウエアとして、実行形式プログラムを直接実行するのではなく、ソースコードをコンパイルして得られたバイトコード（中間コード）が配布され、この配布されたバイトコードをインタプリタによって１命令ずつ解釈して実行するように構成されている。そして、利用者コンピュータ３に配布されるバイトコードは、その一部（暗号区間という）が暗号化されており、暗号区間の復号に必要な復号鍵は、利用者コンピュータ３でのソフトウエアの解釈実行の都度、課金センタ１からネットワーク２を介して利用者コンピュータ３に転送される。また、ソースコードから一部暗号化されたバイトコードを生成し、利用者コンピュータ３に配布するために、開発センタ４が設けられている。開発センタ４から利用者コンピュータ３へのバイトコードの配布は、ネットワークを介してもよいし、ＣＤ－ＲＯＭなどの記録媒体を介してもよい。図１では利用者コンピュータ３が１つしか描かれていないが、当然のことながら、ネットワーク２には多数の利用者コンピュータ３を接続することができる。

【００１４】以下、課金センタ１、利用者コンピュータ３及び課金センタ４の構成について、詳しく説明する。なお、図１において破線で表わされた各構成要素は、本実施の形態における付加的な構成要素である。

【００１５】課金センタ１には、利用者コンピュータ３に配布する復号鍵を格納する鍵格納部１１と、利用者コンピュータ３側からの要求に応じてネットワーク２を介し復号鍵をその利用者コンピュータに送信する復号鍵送信部１２と、課金の集計処理を行う課金集計部１３とが設けられている。さらに、ネットワーク２を介して利用者コンピュータ３がその利用者コンピュータ３でのソフトウエアの使用状況を送信する場合には、この使用状況のデータを受信するために、使用状況受信部１４を課金センタ１内に設ければよい。課金集計部１３は、復号鍵送信部１２での復号鍵の送信の履歴に応じ、使用状況受信部１４が設けられている場合には受信した使用状況のデータに応じ、利用者ごとの課金を集計する。

【００１６】利用者コンピュータ３は、開発センタ４で生成したアプリケーションソフトウエア（課金対象のソフトウエア）のバイトコードを格納するバイトコード格納部３１と、バイトコードを解釈実行するインタプリタ部３２と、バイトコード格納部３１に格納されたバイトコード中の暗号区間を検出する暗号区間検出部３３と、課金センタ１に対して復号鍵の送信を要求しネットワーク２を介して送信されてきた復号鍵を受信する復号鍵受信部３４と、復号鍵受信部３４で受信した復号鍵に基づき、暗号区間検出部３３で検出された暗号区間のバイトコードを復号する復号化部３５とを備えている。この利用者コンピュータ３には、復号化部３５で復号された、暗号区間のバイトコードを一時的に格納する作業領域を設けるようにしてもよい。この作業領域は、例えば利用者コンピュータ３の主記憶メモリ上の領域として確保することができる。また、課金センタ１側にソフトウエアの使用状況を通知するために、復号化部３５での復号処理の実行を検出してソフトウエアの使用状況を検出して記憶する使用状況検出部３７と、検出された使用状況に関するデータを課金センタ１側にネットワークを介して送信するための使用状況送信部３８とを、利用者コンピュータ３内に設けるようにしてもよい。

【００１７】利用者コンピュータ３において、バイトコード格納部３１は、例えば、ハードディスク装置などの記憶装置によって構成される。また、インタプリタ部３２は、暗号区間でない部分のバイトコードについては、バイトコード格納部３１から読み出されたバイトコードをそのまま解釈実行し、暗号区間のバイトコードについては、復号されて復号化部３５から出力されるバイトコード（作業領域３６が設けられている場合は復号され作業領域３６に格納されたバイトコード）を解釈実行する。インタプリタ部３２は、具体的には、バイトコードを１命令ずつ解釈して実行するためのインタプリタと呼ばれるソフトウエアと、インタプリタを実行するＣＰＵ（中央処理装置）などによって、構成される。また、復号鍵受信部３４が復号鍵の送信を要求するのは、例えば、暗号区間を含むバイトコードで表わされるソフトウエアを起動するとき、あるいは、実行中のソフトウエアのバイトコードで暗号区間を検出したとき、などである。

【００１８】利用者コンピュータ３は、パーソナルコンピュータなどの形態をとるものであって、ここでは具体的には図示していないが、キーボードやマウスなどの入力手段、液晶ディスプレイやＣＲＴなどの出力手段、インタプリタ部３２の構成要素ともなるＣＰＵ、さらには、メモリ、各種の記憶装置などを備えている。

【００１９】開発センタ４は、ソースコードを格納する

ソースコード格納部４１と、ソースコード格納部４１に格納されたソースコードをコンパイルしてバイトコードとするコンパイル部４２と、コンパイル部４２の指示によってバイトコードの一部の暗号化処理を行う暗号化部４３と、生成したバイトコードを格納するバイトコード格納部４４とを備えている。暗号化部４３での暗号化に対応する復号鍵が、課金センタ１の鍵格納部１１に格納される。バイトコードでの暗号区間の指定は、ソースコードに、暗号区間の開始や終了を示すソースコードを記述することで行い、コンパイル部４２は、このようなソースコードを検出した場合、暗号区間の開始や終了を表わすバイトコードを生成するとともに、この区間内のバイトコードを暗号化部４３に渡して暗号化させ、暗号化後のバイトコードをバイトコード格納部４４内に格納する。

【００２０】以上説明したシステムにおいて、復号鍵受信部３４は復号鍵取得手段であり、暗号区間検出部３３は暗号区間検出手段であり、復号化部３５は復号手段であり、インタプリタ部３２はインタプリタ手段であり、使用状況検出部３７及び使用状況送信部３８は使用記録検出手段である。さらに、コンパイル部４２がコンパイル手段であり、暗号化部４３が暗号化手段である。

【００２１】次に、上述したソフトウエアの保護方式の動作について、具体的な実施例を用いて説明する。

【００２２】《実施例１》実施例１は、基本構成、すなわち、使用状況受信部１４や作業領域３６、使用状況検出部３７、使用状況送信部３８を含まない構成についてのものである。実施例１での処理の流れが図２に示されている。

【００２３】課金対象のソフトウエアが、予めバイトコードとして利用者コンピュータ３のバイトコード格納部３１に格納されている。このバイトコードでは、予め一部が暗号化されており、上述したように、暗号区間の開始及び終了を示すバイトコードが埋め込まれている。暗号区間は１箇所または複数箇所存在するが、ここでは、暗号区間が複数箇所存在する場合でも、復号のための復号鍵は１種類であるとする。

【００２４】利用者コンピュータ３では、課金対象のアプリケーションソフトウエアが起動されると（ステップ１０１）、復号鍵受信部３４が、このソフトウエアの実行前に、ネットワーク２を介し、課金センタ１からこのソフトウエアの復号鍵を取得する（ステップ１０２）。復号鍵の配送には、適切な認証及び暗号化を実施するものとする。暗号区間検出部３３は、暗号区間が開始したかどうか、すなわち暗号区間開始を表わすバイトコード（暗号区間開始バイトコード）があるかを常時監視している（ステップ１０３）。暗号区間開始でない場合には、インタプリタ部３２が、１命令ずつバイトコードをバイトコード格納部３１から読み出し、解釈実行し（ステップ１０４）、そののちステップ１０３に戻る。ステップ１０４を含むループは、暗号区間開始バイトコードを検出するまで繰り返される。

【００２５】ステップ１０３で暗号区間開始バイトコードを検出した場合、すなわち暗号区間が開始した場合には、暗号区間検出部３３は、暗号区間終了であるかどうか、すなわち暗号区間終了を示すバイトコード（暗号区間終了バイトコード）を常時監視する（ステップ１０５）。暗号区間終了であればステップ１０３に戻り、暗号区間終了でなければ、復号化部３５が、課金センタから復号鍵受信部３４が取得した復号鍵を用いて、１命令ずつ読み出されたバイトコードを復号し（ステップ１０６）、このように復号されたバイトコードをインタプリタ部３２が解釈実行し（ステップ１０７）、ステップ１０５に戻る。このステップ１０６及びステップ１０７を含むループは、暗号区間終了バイトコードを検出するまで、すなわち暗号区間終了を検出するまで繰り返される。

【００２６】結局、暗号区間終了バイトコードを検出した場合には、暗号区間開始バイトコードを再度検出するまで、復号を行うことなしに、インタプリタ部３２が１命令ずつバイトコードを読み出して解釈実行する。

【００２７】以上、利用者コンピュータ３での処理を説明したが、このとき、課金センタ１では、復号鍵送信部１２による復号鍵の送信履歴に基づき、課金集計部１３が利用者ごとの課金処理を実行する。

【００２８】《実施例２》実施例１ではアプリケーションプログラムごとに１つの復号鍵が用いられていたが、この実施例２は、アプリケーションプログラムのバイトコード中に複数の暗号区間が設定されるとともに、典型的には暗号区間ごとに異なる復号鍵を用いることにより、全体として複数の復号鍵が用いられていることで、実施例１と異なっている。暗号区間ごとにそこで使用すべき復号鍵を特定するために、暗号区間開始バイトコードには暗号区間を識別する暗号区間ＩＤが埋め込まれており、暗号区間ＩＤとその暗号区間を復号するための復号鍵が対で管理されている。その他の点では、この実施例２は実施例１と同様の構成である。実施例２での処理の流れが図３に示されている。

【００２９】利用者コンピュータ３では、課金対象のアプリケーションソフトウエアが起動されると（ステップ１１１）、復号鍵受信部３４が、このソフトウエアの実行前に、ネットワーク２で接続された課金センタ１から、暗号区間ＩＤと対応付けられた復号鍵を複数個一括して取得する（ステップ１１２）。暗号区間検出部３３は、暗号区間が開始したかどうかを常時監視しており（ステップ１１３）、暗号区間開始でない場合は、実施例１と同様に、インタプリタ部３２は、１命令ずつバイトコードを解釈実行し（ステップ１１４）、ステップ１１３に戻る。

【００３０】ステップ１１３で暗号区間が開始した場合

には、復号鍵受信部３４は、暗号区間開始バイトコードで指定された暗号区間ＩＤに対応した復号鍵を選択する（ステップ１１５）。そして、暗号区間終了であるかどうかが判断され（ステップ１１６）、暗号区間終了であればステップ１１３に戻り、暗号区間終了でなければ、復号化部３５が、ステップ１１５で選択された復号鍵によって、１命令ずつ読み出されたバイトコードを復号し（ステップ１１７）、復号されたバイトコードをインタプリタ部３２が解釈実行し（ステップ１１８）、ステップ１１６に戻る。このステップ１１７及びステップ１１８を含むループは、暗号区間終了を検出するまで繰り返される。

【００３１】この実施例２でも、課金センタ１では、復号鍵送信部１２による復号鍵の送信履歴に基づき、課金集計部１３が利用者ごとの課金処理を実行する。

【００３２】《実施例３》この実施例３は、実施例２と同様のものであるが、アプリケーションソフトウエアの実行開始後に暗号区間ごとの復号鍵をその都度取得する点で、実施例２と異なっている。実施例３での処理の流れが図４に示されている。この実施例３でも、アプリケーションソフトウエアには複数の暗号区間が設定され、それぞれ異なる暗号区間ＩＤで特定される複数の復号鍵が使用され、暗号区間ＩＤが暗号区間開始バイトコードに埋め込まれている。

【００３３】利用者コンピュータ３では、課金対象のアプリケーションソフトウエアが起動されると（ステップ１２１）、そのまま、このアプリケーションプログラムの実行が開始される。暗号区間検出部３３は、暗号区間が開始したかどうかを常時監視しており（ステップ１２２）、暗号区間開始でない場合は、実施例１と同様に、インタプリタ部３２が１命令ずつバイトコードを解釈実行し（ステップ１２３）、ステップ１２２に戻る。

【００３４】ステップ１２２で暗号区間が開始が検出された場合には、復号鍵受信部３４が、暗号区間開始バイトコードで指定された暗号区間ＩＤに対応した復号鍵の送信を課金センタ１側に要求し、その鍵を取得する（ステップ１２４）。そして、暗号区間終了であるかどうかが判断され（ステップ１２５）、暗号区間終了であればステップ１２２に戻り、暗号区間終了でなければ、復号化部３５が、ステップ１２４で取得された復号鍵によって、１命令ずつ読み出されたバイトコードを復号し（ステップ１２６）、復号されたバイトコードをインタプリタ部が解釈実行し（ステップ１２７）、ステップ１２５に戻る。このステップ１２６及びステップ１２７を含むループは、暗号区間終了を検出するまで繰り返される。

【００３５】この実施例３では、暗号区間ＩＤで特定される暗号区間ごとの復号鍵の送信履歴に基づき、課金集計部１３での利用者ごとの課金処理が実行される。したがって、アプリケーションプログラムに複数の機能が含まれているとして、各機能ごとの使用頻度に応じた課金が可能となる。具体的には、利用者は、その使用しなかった機能に対する使用量を払う必要がなくなる。

【００３６】《実施例４》実施例１では、復号鍵を用いた復号の際、バイトコードの１命令ごとに、復号と解釈実行が行われている（図１のステップ１１７、１１８のループ）。これに対し、この実施例４では、暗号区間を検出したらその暗号区間内のバイトコードを一括して復号して作業領域３６に格納し、その後、インタプリタ部３２が復号されたバイトコードを１命令ずつ実行する。その他の点では、実施例４は実施例１と同様の構成であり、復号鍵の種類は、暗号区間が複数ある場合でも、１つである。図５は実施例４での処理を示す流れ図である。

【００３７】利用者コンピュータ３では、アプリケーションソフトウェアが起動されると（ステップ１３１）、復号鍵受信部３４が、このソフトウェアの実行前に、ネットワーク２で接続された課金センタ１から、復号鍵を取得する（ステップ１３２）。暗号区間検出部３３は、暗号区間が開始したかどうかを常時監視しており（ステップ１３３）、暗号区間開始でない場合は、実施例１と同様に、インタプリタ部３２が１命令ずつバイトコードを解釈実行して（ステップ１３４）、ステップ１３３に戻る。

【００３８】ステップ１３３で暗号区間の開始を検出した場合には、暗号区間の終了となったかどうかを常時監視するようにし（ステップ１３５）、暗号区間終了でない場合には、復号鍵受信部３４が受信した復号鍵に基づいて、復号化部３２が１命令ずつバイトコードを復号し（ステップ１３６）、復号したバイトコードを作業領域３６内に格納し（ステップ１３７）、ステップ１３５に戻る。すなわち、暗号区間終了となるまで、ステップ１３５～１３７のループが繰返し実行され、その暗号区間のバイトコードが一括して復号されて作業領域３６内に格納されることになる。そして、ステップ１３５で暗号区間終了を検出したら、今度はインタプリタ部３２が作業領域３６から１命令ずつバイトコードを取り出し（ステップ１３８）、作業領域３６から取り出したバイトコードが暗号区間終了バイトコードであるかどうかを判断する（ステップ１３９）。暗号区間終了バイトコードでなければ、インタプリタ部３２は、作業領域３６から取り出した１命令分のバイトコードを解釈実行し（ステップ１４０）、ステップ１３８に戻る。すなわち、インタプリタ部３２は、作業領域３６内の復号されたバイトコードを連続して解釈実行する。ステップ１３９で暗号区間終了を検出した場合には、ステップ１３３に戻る。

【００３９】この実施例４では、暗号区間ごとにバイトコードを一括して復号して作業領域３３に格納するので、バイトコードの復号に伴うスループットを向上させることができる。

【００４０】《実施例５》上述の各実施例では、復号鍵

の配送に着目して課金処理を行っているが、この実施例５では、課金センタ１内に使用状況受信部１４を設け、利用者コンピュータ３内に使用状況検出部３７と使用状況送信部３８を設け、利用者コンピュータ３から課金センタ１にネットワークを介して送信される使用状況データに基づいて、課金処理が行われるようにしている。ここでは、実施例１と同様に、復号鍵の種類は１種類であって、ソフトウエアの実行前に復号鍵受信部３４が復号鍵を取得するものとする。実施例５での処理の流れが図６に示されている。

【００４１】利用者コンピュータ３では、課金対象のアプリケーションソフトウェアが起動されると（ステップ１５１）、復号鍵受信部３４が、このソフトウェアの実行前に、ネットワーク２で接続された課金センタ１から、復号鍵を取得する（ステップ１５２）。暗号区間検出部３３は、暗号区間が開始したかどうかを常時監視しており（ステップ１５３）、暗号区間開始でない場合は、実施例１と同様に、インタプリタ部３２が、１命令ずつバイトコードを解釈実行し（ステップ１５４）、ステップ１５３に戻る。

【００４２】ステップ１５３で暗号区間が開始した場合には、使用状況検出部３７がソフトウエアの使用記録を取得し、記憶する（ステップ１５５）。そして、暗号区間終了であるかどうかが判断され（ステップ１５６）、暗号区間終了であればステップ１５３に戻り、暗号区間終了でなければ、復号化部３５が、復号鍵受信部３４によって取得した復号鍵によって、１命令ずつ読み出されたバイトコードを復号し（ステップ１５７）、復号されたバイトコードをインタプリタ部３２が解釈実行し（ステップ１５８）、ステップ１５６に戻る。このステップ１５７及びステップ１５８を含むループは、暗号区間終了を検出するまで繰り返される。

【００４３】一方、使用状況検出部３７で取得され記憶された使用状況のデータは、使用状況受信部３８により、上記処理とは非同期に例えば所定の期間ごとに、ネットワーク２を介して課金センタ１の使用状況受信部１４に送信される（ステップ１５９）。課金センタ１では、受信した使用状況データによって、利用者ごとの課金処理が実行される。

【００４４】この実施例５では、復号鍵の配送ごとに課金処理を行う必要がないので、課金センタ１での処理が軽減される。

【００４５】《実施例６》この実施例６は、開発センタ４での処理に係るものである。図７は実施例６での処理を示す流れ図である。

【００４６】ソースコード格納部４１にはソースコードが格納されており、ソースコード中では、暗号区間の開始と終了とがそれぞれ暗号区間開始ソースコードと暗号区間終了ソースコードで示されているものとする。ソースコードのコンパイルが開始すると（ステップ１６１）、コンパイル部４２は、ソースコードをバイトコードに変換する（ステップ１６２）。その際、暗号区間開始ソースコード及び暗号区間終了ソースコードは、それぞれ、暗号区間開始バイトコード及び暗号区間終了バイトコードに変換される。そして、暗号化部４３により、予め指定された暗号鍵を用いて、暗号区間開始バイトコードと暗号区間終了バイトコードとの間の区間、すなわち暗号区間のバイトコードを暗号化する（ステップ１６３）。このように一部が暗号化されたバイトコードは、バイトコード格納部４４内に格納され、ネットワークやＣＤ－ＲＯＭなどを用いて、利用者コンピュータ３に配布される。また、上記の暗号鍵に対応する復号鍵は、課金センタ１の鍵格納部１１内に格納される。

【００４７】

【発明の効果】以上説明したように本発明によれば、利用者コンピュータにおいて、いずれの時点においても、暗号化されていない部分を含まないソフトウェアがハードディスク等の記憶媒体上に存在しない。このため、ソフトウェアの不正な反復使用を確実に阻止することができ、著作権者はソフトウェアの使用のつど確実に使用料を徴収することが可能になり、ユーザにとっても必要な機能のみを安価な使用料で使用することが可能になるという効果がある。また、ソフトウェアの暗号化に用いる暗号鍵の個数と暗号化の範囲を選択することにより、起動するソフトウェアの単位で課金することも、起動するソフトウェア内の機能単位に課金することも可能となる。

【００４８】暗号区間の復号による性能低下は、暗号区間全体を一度に復号して作業記憶に格納することにより、軽減できる。さらに、暗号区間に入った時点で使用記録を取得し、ソフトウェア使用終了後あるいは一定期間間隔で使用記録を課金センタに送付することにより、きめ細かい使用記録に基づく課金が、課金センタとの通信のオーバヘッドを増やすことなく実現可能となる。

【００４９】さらにまた、コンパイラに暗号区間開始／終了のソースコードを解釈し暗号化する機能を付加することにより、高い保護特性を持つソフトウェアの自動生成が可能となる。

【図面の簡単な説明】

【図１】本発明の実施の一形態のソフトウエアの保護方式の構成を示すブロック図である。

【図２】実施例１での利用者コンピュータにおける処理を説明する流れ図である。

【図３】実施例２での利用者コンピュータにおける処理を説明する流れ図である。

【図４】実施例３での利用者コンピュータにおける処理を説明する流れ図である。

【図５】実施例４での利用者コンピュータにおける処理を説明する流れ図である。

【図６】実施例５での利用者コンピュータにおける処理

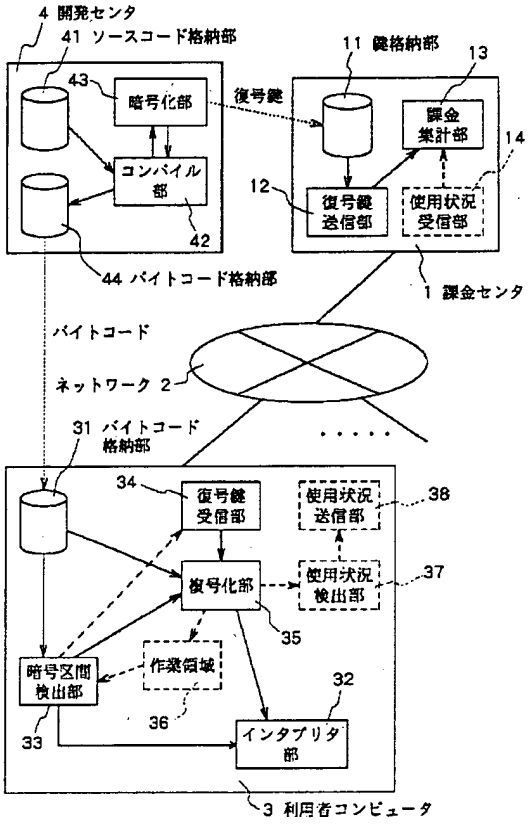
を説明する流れ図である。

【図７】実施例６での開発センタにおける処理を説明する流れ図である。

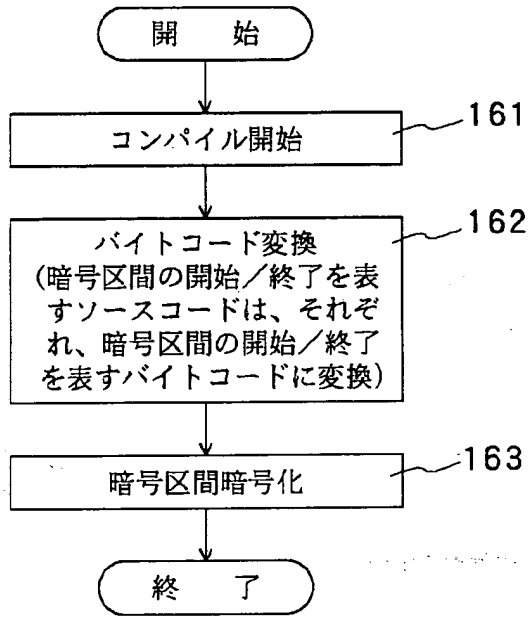
【符号の説明】

１　課金センタ
２　ネットワーク
３　利用者コンピュータ
４　開発センタ
１１　鍵格納部
１２　復号鍵送信部
１３　課金集計部
１４　使用状況受信部
３１，４４　バイトコード格納部
３２　インタプリタ部
３３　暗号区間検出部
３４　復号鍵受信部
３５　復号化部
３６　作業領域
３７　使用状況検出部
３８　使用状況送信部
４１　ソースコード格納部
４２　コンパイル部
４３　暗号化部
１０１～１０７，１１１～１１８，１２１～１２７　ステップ
１３１～１４０，１５１～１５９，１６１～１６３　ステップ

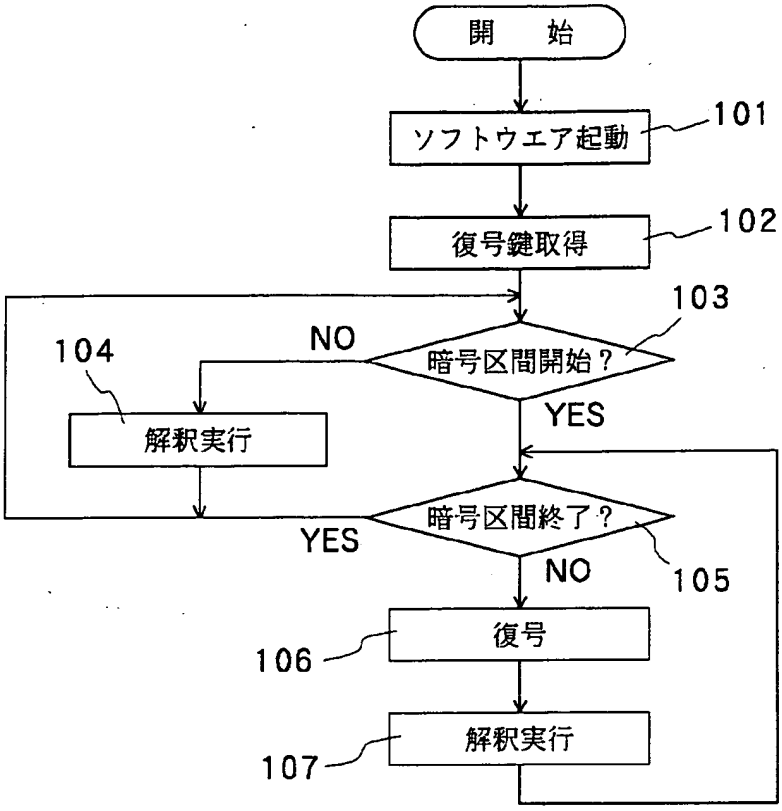
【図１】



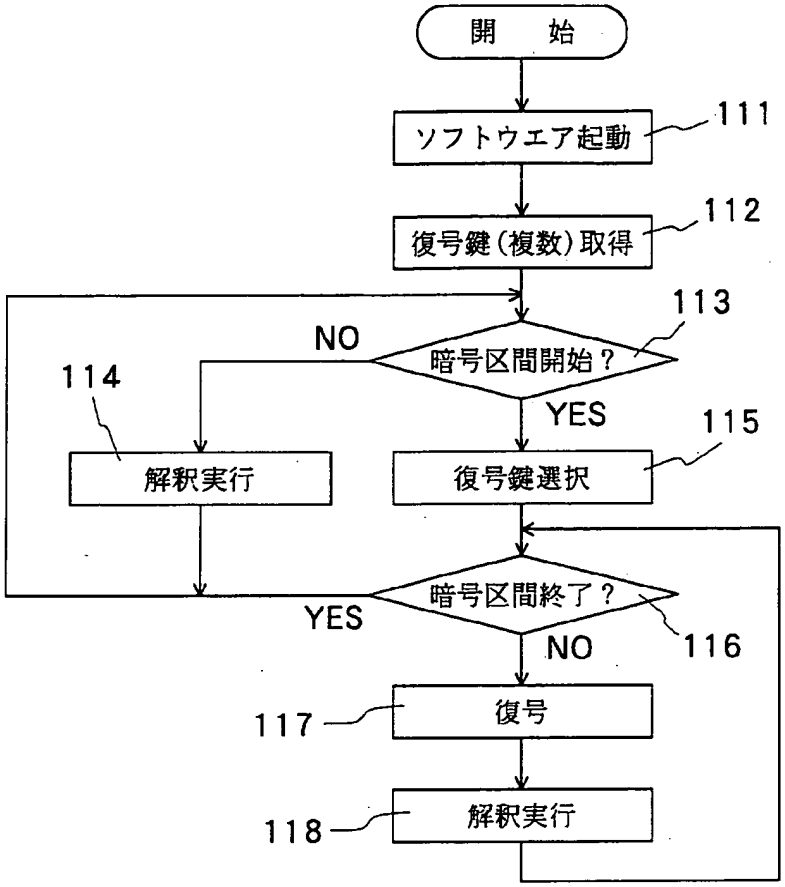
【図７】



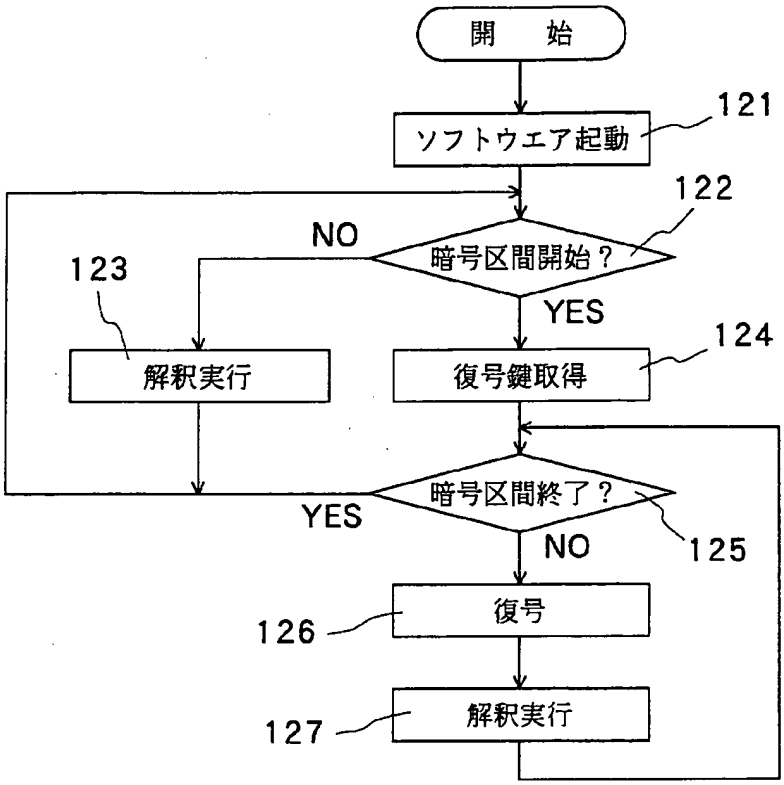
【図２】


開　始
ソフトウエア起動
101
復号鍵取得
102
103
暗号区間開始？
NO
104
解釈実行
YES
暗号区間終了？
YES
NO
105
復号
106
解釈実行
107

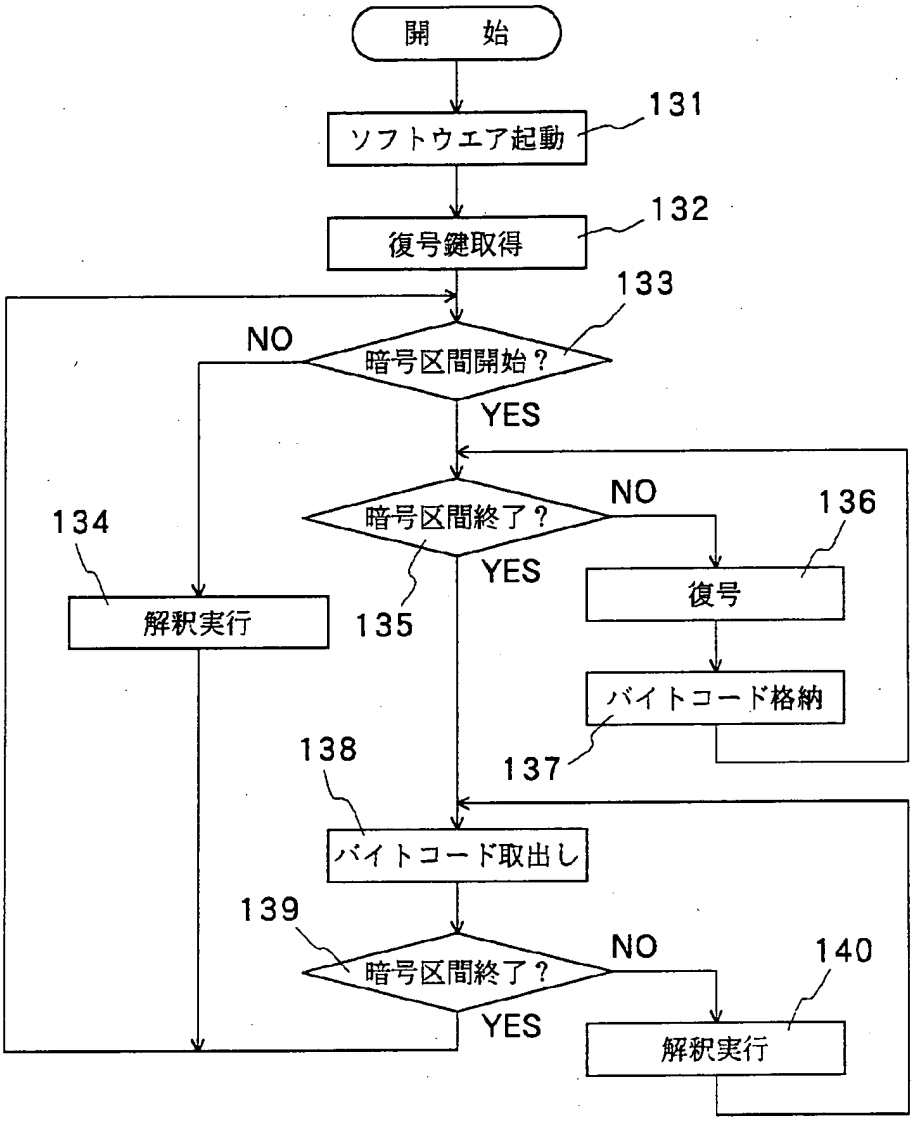
【図3】


開　始
ソフトウエア起動
111
復号鍵(複数)取得
112
暗号区間開始？
113
NO
114
YES
115
解釈実行
復号鍵選択
暗号区間終了？
YES
NO
116
復号
117
解釈実行
118

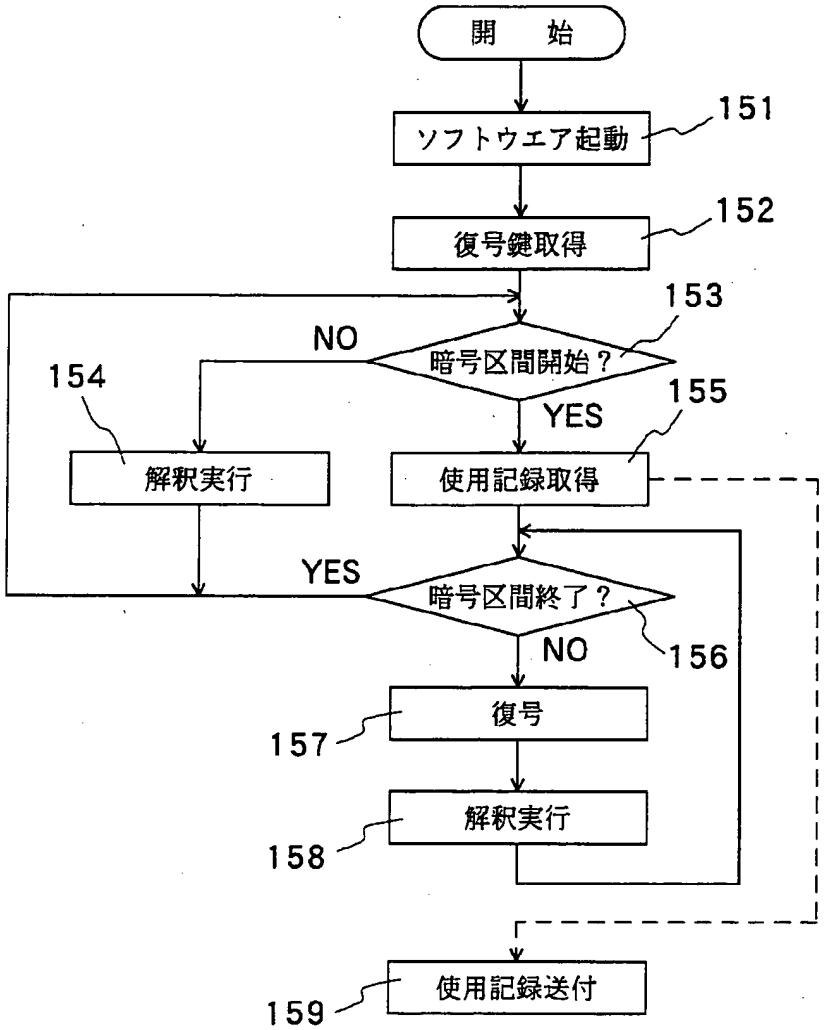
【図４】


開　始
ソフトウエア起動
121
暗号区間開始？
122
NO
123
YES
解釈実行
復号鍵取得
124
暗号区間終了？
YES
NO
125
復号
126
解釈実行
127

【図５】


開　始
ソフトウエア起動
131
復号鍵取得
132
暗号区間開始？
133
NO
YES
暗号区間終了？
NO
YES
134
136
135
解釈実行
復号
バイトコード格納
137
138
バイトコード取出し
139
暗号区間終了？
NO
YES
140
解釈実行

【図6】


開　始
ソフトウエア起動
151
復号鍵取得
152
暗号区間開始？
153
NO
154
YES
155
解釈実行
使用記録取得
暗号区間終了？
YES
156
NO
復号
157
解釈実行
158
使用記録送付
159